CLAIMS

1. An encryption communication system for secret message communication, comprising an encryption transmission apparatus and an encryption reception apparatus, wherein

the encryption transmission apparatus includes:

a storage unit that stores therein one message;

an encryption unit operable to perform an encryption computation on the message a plural number of times, thereby generating ciphertexts equal in number to the number of times of the encryption computation;

a computation unit operable to perform a one-way operation on the message, thereby generating a comparison computation value; and

a transmission unit operable to transmit the ciphertexts and the comparison computation value, and

the encryption reception apparatus includes:

a reception unit operable to receive the ciphertexts and the comparison computation value;

a decryption unit operable to perform a decryption computation, which corresponds to the encryption computation, on each of the ciphertexts, thereby generating decrypted messages equal in number to the number of the ciphertexts;

a computation unit operable to perform the one-way operation on each of the decrypted messages, thereby generating decryption computation values equal in number to the number of the decrypted messages; and

a judging unit operable to compare the decryption computation values with the received comparison computation value, and i) if at least one of the decryption computation values matches the received comparison computation value, output a corresponding decrypted message as a correct decrypted text, and ii) if none of the decryption computation values matches the received comparison computation value, output a decryption error.

2. The encryption communication system of Claim 1, wherein

the encryption computation used by the encryption unit conforms to NTRU cryptosystem, and

the decryption computation used by the decryption unit conforms to the NTRU cryptosystem.

3. An encryption transmission apparatus for secret message communication, comprising:

a storage unit that stores therein one message;

an encryption unit operable to perform an encryption computation on the message a plural number of times, thereby generating ciphertexts equal in number to the number of times of the encryption computation;

a computation unit operable to perform a one-way operation on the message, thereby generating a comparison computation value; and

a transmission unit operable to transmit the ciphertexts and the comparison computation value.

4. The encryption transmission apparatus of Claim 3, wherein

the encryption unit comprises:

an encryption computation subunit operable to perform an invertible data conversion on the message thereby generating a converted message, and perform an encryption algorithm on the converted message thereby generating a ciphertext; and

a repetition control subunit operable to control the encryption computation subunit to repeat the generation of converted message and the generation of ciphertext, the plural number of times.

5. The encryption transmission apparatus of Claim 4, wherein

the encryption computation subunit generates a random number of fixed length, and generates the converted message by adding the random number to the message.

6. The encryption transmission apparatus of Claim 5, wherein

the encryption algorithm used by the encryption computation subunit conforms to NTRU cryptosystem.

7. An encryption reception apparatus for secret message communication, where the encryption transmission apparatus stores therein one message, performs an encryption computation on the message a plural number of times thereby generating ciphertexts equal in number to the number of the encryption computation, performs a one-way operation on the message thereby generating a comparison computation value, and transmits the ciphertexts and the comparison computation value, the encryption reception apparatus comprising:

a reception unit operable to receive the ciphertexts and the comparison computation value;

a decryption unit operable to perform a decryption computation, which corresponds to the encryption computation, on each of the ciphertexts, thereby generating decrypted messages equal in number to the number of the ciphertexts;

a computation unit operable to perform the one-way operation on each of the decrypted messages, thereby generating decryption computation values equal in number to the number of the decrypted messages; and

a judging unit operable to compare the decryption computation values with the received comparison computation value, and i) if at least one of the decryption computation values matches the received comparison computation value, output a corresponding decrypted message as a correct decrypted text, and ii) if none of the decryption computation values matches the received comparison computation value, output a decryption error.

8. The encryption reception apparatus of Claim 7, wherein

the encryption transmission apparatus performs an invertible data conversion on the message thereby generating a converted message, performs an encryption algorithm on the converted message thereby generating a ciphertext, and repeats the generation of converted message and the generation of ciphertext, the plural number of times, and wherein

the decryption unit comprises:

a decryption computation subunit operable to perform a decryption algorithm, which corresponds to the encryption algorithm, on a ciphertext thereby generating a decrypted text, and perform an inverse conversion of the invertible data conversion on the decrypted text thereby generating a decrypted message; and a repetition control subunit operable to control the decryption computation subunit to repeat the generation of decrypted content and the generation of decrypted message, the plural number of times.

9. The encryption reception apparatus of Claim 8, wherein

the encryption transmission apparatus generates a random number of fixed length, and generates the converted message by adding the random number to the message, and wherein

the decryption computation subunit generates the decrypted message by removing the random number of fixed length from the decrypted content.

10. The encryption reception apparatus of Claim 9, wherein

the encryption algorithm used by the encryption transmission apparatus conforms to NTRU cryptosystem, and wherein

the decryption algorithm used by the decryption computation subunit conforms to the NTRU cryptosystem.

11. An encryption transmission method used in an encryption transmission apparatus that stores therein one message and transmits the message in secrecy, the encryption transmission method comprising:

an encryption step of performing an encryption computation on the message a plural number of times, thereby generating ciphertexts equal in number to the number of times of the encrypted computation;

a computation step of performing a one-way operation on the message, thereby generating a comparison computation value; and

a transmission step of transmitting the ciphertexts and the comparison computation value.

12. An encryption transmission program used in an encryption transmission apparatus that stores therein one message and transmits the message in secrecy, the encryption transmission program comprising:

an encryption step of performing an encryption computation on the message a plural number of times, thereby generating ciphertexts equal in number to the number of times of the encrypted computation;

a computation step of performing a one-way operation on the message, thereby generating a comparison computation value; and

a transmission step of transmitting the ciphertexts and the comparison computation value.

13. The encryption transmission program of Claim 12, being

recorded in a computer-readable recording medium.

14. An encryption reception method used in an encryption reception apparatus that receives a message from an encryption transmission apparatus in secrecy, where the encryption transmission apparatus stores the message therein, performs an encryption computation on the message a plural number of times thereby generating ciphertexts equal in number to the number of times of the encryption computation, performs a one-way operation on the message thereby generating a comparison computation value, and transmits the ciphertexts and the comparison computation value, the encryption reception method comprising:

a reception step of receiving the ciphertexts and the comparison computation value;

a decryption step of performing a decryption computation, which corresponds to the encryption computation, on each of the ciphertexts, thereby generating decrypted messages equal in number to the number of the ciphertexts;

a computation step of performing the one-way operation on each of the decrypted messages, thereby generating decryption computation values equal in number to the number of the decrypted messages; and

a judging step of comparing the decryption computation values with the received comparison computation value, and i) if at least one of the decryption computation values matches the received comparison computation value, outputting a corresponding decrypted message as a correct decrypted text, and ii) if none of the decryption computation values matches the received comparison computation value, outputting a decryption error.

15. An encryption reception program used in an encryption reception apparatus that receives a message from an encryption transmission apparatus in secrecy, where the encryption transmission apparatus stores the message therein, performs an encryption computation on the message a plural number of times thereby generating ciphertexts equal in number to the number of times of the encryption computation, performs a one-way operation on the message thereby generating a comparison computation value, and transmits the ciphertexts and the comparison computation value, the encryption reception program comprising:

a reception step of receiving the ciphertexts and the comparison computation value;

a decryption step of performing a decryption computation, which corresponds to the encryption computation, on each of the ciphertexts, thereby generating decrypted messages equal in number to the number of the ciphertexts;

a computation step of performing the one-way operation on each of the decrypted messages, thereby generating decryption computation values equal in number to the number of the decrypted messages; and

a judging step of comparing the decryption computation values with the received comparison computation value, and i) if at least one of the decryption computation values matches the received comparison computation value, outputting a corresponding decrypted message as a correct decrypted text, and ii) if none of the decryption computation values matches the received comparison computation value, outputting a decryption error.

16. The encryption reception program of Claim 15, being recorded in a computer-readable recording medium.